Chapter 12
NETWORK MANAGEMENT

1201 INTRODUCTION

Network Management is the process of controlling a complex data network to maximise its efficiency and productivity. It is therefore a critical aspect for any wide area network.

1202 AIM

The aim of this chapter is to provide guidance for the Network Management of a maritime tactical WAN.

1203 OVERVIEW

a. Network Management (NM), which includes configuration, performance, fault and security management, takes place within nodes (i.e. LAN) and throughout the wider network (i.e. WAN)

b. From a WAN perspective, NM is commonly associated with the duties and responsibilities of a Network Operations Centre (NOC). A NOC while logically in one location, could physically be in a number of locations (i.e. distributive in nature).

c. Depending on the design of the MTWAN, there will be a number of NOCs. There will normally be three types of NOCs Primary NOC, National NOC, and Node Level NOC.

1204 NM ARCHITECTURE (HIERARCHY)

a. **Primary NOC.** The MTWAN NOC or primary NOC provides a single point of contact for network services within a maritime tactical network. The provision of services to this network and for coordinating connectivity of national NOCs to the network is a MTWAN NOC responsibility.

b. **National NOC.** The national NOCs are responsible for coordinating network services within their national boundaries and to coordinate activities with the primary NOC.

c. **Node Level.** Individual nodes are responsible for management of local network elements. Each platform will have a limited capability to provide

network management services on the LAN and is responsible first to the national NOC and then the primary NOC for overall network services.

1205 NM ELEMENTS

The elements of network management are:

a. Configuration Management which controls the behaviour of the network and can be considered to comprise:

(1) Configuration, monitoring and control of routers, other SNMP-managed network devices and CAP/CRIU;

(2) Provisioning, bandwidth management and monitoring;

(3) Route Policy Management (which networks carry transit traffic, diversity routing, tunnelling and overlay network management, security service levels for routing protocols, etc.); and

(4) Management of DNS, network time service, and other required infrastructure services

b. Performance Management which measures the performance of the network hardware, software and media. It comprises:

(1) Monitoring of Links, Routers, network connectivity and Services;

(2) Net loading, congestion control monitoring;

(3) Performance optimisation for bandwidth-disadvantaged users;

(4) Service Prioritisation;

c. Fault Management

(1) Fault detection, isolation and troubleshooting;

(2) Fault-logging and analysis.

d. Security Management which control access to information on the network, and can be considered to comprise:

(1) Intrusion detection and response, including co-ordination of multiple detections received from diverse locations;

(2) Vulnerability assessment;

(3) Security Policy Establishment, Monitoring, & Enforcement;

(4) Firewall Management;

(5) Response Centre activities (route attack notifications to CERTs, co-ordinate fixes);

(6) Guard Management ("Guards" = devices connecting 2 or more networks running under different security policies and/or sensitivities, e.g., a guard which connects the US National networks with the MTWAN); and

(7) Encryption Device Management (e.g., TACLANE/FASTLANE Management).

e. Administration which comprise the generation of reports, pertaining to:

(1) Robust Network Management under varying operational conditions (i.e., EMCON);

(2) DNS Co-ordination;

(3) Interface with other non-MTWAN network management entities (e.g., national NOCs and their network management systems);

(4) Provisioning requests up to national NOCs; responses down to MTWAN NOC;

(5) Critical fault alerts/alarms sent up to national NOCs; and

(6) Configuration and performance summary status/statistics sent up to national NOCs.

1206 REMOTE OR LOCAL MANAGEMENT

a. Centralised, remote management of the MTWAN elements by a NOC will be more efficient than co-ordinated local control. Remote management reduces the need for additional skilled staff on each mobile unit, minimises the risk of errors in configuration, and permits rapid reaction to events. However, the capability for remote management is limited at present by national policy.

b. National policies may prohibit remote control of network elements for safety or system integrity reasons. Monitoring may be acceptable, if specific

equipment items can be configured to respond to remote requests for status information but ignore control messages. Network management procedures and protocols must be secure.

1207 GENERATION OF REPORTS

An MTWAN NOC will provide network status information to the CTF, to network members and to the higher level Allied WAN management system. This information must be kept current and will be presented as a Web page. To enable an MTWAN NOC to collect and collate the latest status information, all platform network managers are to provide local status reports on a regular basis (or at least, when there has been any change since the last report). The NOC will compile these into an overall status report.

1208 SECURITY RESPONSIBILITY

The MTWAN NOC should provide a capability for intrusion detection, primarily to minimise unauthorised traffic over the MTWAN.

1209 TOOLS

Several tools are available to facilitate network status and traffic load monitoring, as well as tools using SNMP to implement centralized or remote control of network elements. All platforms should, as a minimum, have the ability to monitor local network status and traffic performance.

Annex A to Chapter 12 to ACP 200

NETWORK MANAGEMENT SOP

12A01 INTRODUCTION

The management of an MTWAN involves monitoring the operation of application servers (ie Domino, Sametime and mail servers), network servers (i.e. DNS and multicast transport protocols) and network devices (i.e. routers). Network Management (NM) also includes the collection and analysis of network statistics to assist with troubleshooting of network or application problems, network optimisation and future planning.

12A02 AIM

The aim of this Annex is to provide the standard operating procedures for managing an MTWAN Network.

12A03 SCOPE

NM services to be supported within a typical MTWAN will be limited to:

- Gathering LAN and WAN traffic statistics to support future planning and network optimisation;
- Monitoring the health of network devices and application servers;
- Monitoring the operation of network services and C2 applications;
- Identifying network changes; and
- Troubleshooting network and application problems.

12A04 NETWORK MANAGEMENT TOOLS

Simple Network Management Protocol (SNMP), an Internet Protocol, is the principal means employed to conduct NM. SNMP defines a set of parameters that a network manager can query (Management Information Base), the format of NM messages and the rules by which these messages are exchanged. *Openview* and *Network Node Manager* from *HP*, *Tivoli Netview* from *IBM*, *Spectrum* from *Aprisma* and *WhatsUpGold* from *Ipswitch* are common commercial tools that have been successfully employed in MTWANs. These tools have different capabilities, and user interfaces. Selection and installation of NM tools will be a national issue

12A05 NETWORK MANAGEMENT STRATEGY

a. A MTWAN NOC will be operated on a 24/7 basis. The MTWAN Network manager will be responsible for the following:
   - Configuration of routers, servers and user workstations;
   - Installation of NM station;
   - Installation of applications and network services;
   - Configuration of WAN links including CAP/CRIU, radio

- Configuration of cryptographic equipment;
- Configuration of applications and network in support of EMCON; and
- Collection of local network statistics.

b. Network statistics will normally include protocol distribution; packet and byte counts sorted by protocol or by host, connection matrices, and error counts on different protocol layers.

c. Unit network managers must ensure that network devices, application servers, clients, and WAN interfaces on the local network have been correctly configured and remain functional.

d. NM stations will be capable of processing SNMP traps (unsolicited messages sent by an SNMP-enabled host indicating it is not fully operational) received from local hosts. The NM stations are to be configured to automatically generate audible alarms and notification messages whenever a trap is received.

e. The MTWAN NOC will manage AS Border Routers, network services (such as DNS, mail server, and multicast transport applications) and application servers (such as Domino and Sametime) for the MNTG.

f. Performance of the local network and its hosts must be continuously monitored. An automatic alert will be generated when warning or critical threshold limits for the network (such as error rates) or computing resources (such as memory and disk space) have been reached (or are being approached).

g. Under the direction or co-ordination of the MTWAN NOC, unit network managers will assist with the analysis and resolution of network and application problems as required.

h. Network bottlenecks are most likely to occur on low speed RF links and therefore NM traffic over these links must be kept to a minimum. A unit NM station shall only discover and manage hosts on its local network. No traffic generated by the local automated NM processes (such as network discovery) must be allowed to travel further than the unit's Area Border router.

i. The NOC will monitor and provide a consolidated view of the health of the network backbone (Area 0). The view will also include the status of MNTG application servers. The view will be updated at least every 30 minutes and be accessible to units network managers via a Web browser.

j. Under the direction or co-ordination of the NOC, units network managers will conduct the analysis of network statistics to identify potential problems, and to

anticipate and plan for additional hosts and services.

k. An FTP server is to be provided at the NOC to support the collection and storage of software and configuration information for all configurable network devices and services within the MTWAN in support of a specific exercise or operation.

12A06 NETWORK MANAGEMENT TOOLS SET -UP

a. To establish NM tools discussed above, the following installation and set-up is required:

(1) Install Mchat (a multicast text chat for use by network managers).

(2) Select a suitable computer to be the NM station and install NM software. If the computer is being used for other applications, ensure that these will not be affected by the NM functionality.

(3) Set up a Web server on the NM station to let users view the NM information using a Web browser. Enable Web server security to grant users “read-only” access to the Web pages.

(4) Enable SNMP on all hosts and set their “read-only” Community Name (editing SNMP Agent’s Management Information Base {MIB} is not allowed).

(5) Use the “Lookup” tool provided by the NM software to resolve IP addresses and names (forward and reverse mapping) of the local hosts using DNS. Rectify any DNS problems encountered.

(6) Enable the Network Mapping function of the NM to discover the local network up to the local Area Border routers and generate a topology map. The map will include all the active interfaces of the routers. Set the default polling interval for the network discovery and monitoring to 30 minutes. For routers and servers, which are critical components of the network, *the polling interval should be set to no longer than 10 minutes.*

(7) Enable the monitoring function of the NM software to monitor the status of local hosts, the services running on those hosts and the WAN links. Colours and symbols will be used to indicate any changes to the network.

(8) Enable the collection of local network statistics.

12A07 TROUBLESHOOTING

a. The most common problems that occur in an operational IP network are:
   - Slow Responses;
   - Connectivity Problems; and
   - Application Problem.

b. Slow Responsiveness

   (1) When an application is running slowly, the cause of the problem may be a congested network or an overloaded server.

   (2) Use NM tools to collect and analyse network statistics to determine whether the network is congested. If it is, identify hosts and applications that are causing the congestion and then co-ordinate with the NOC to shut down non-essential bandwidth users.

   (2) Request the network manager of the remote server to determine whether the server has too many clients and therefore it is overloaded, and then contact the NOC for problem resolution.

b. Connectivity Problem

   (1) When connection to a remote server cannot be established, the problem may be caused by one of the following: DNS; unreachable host; or routing.

   (2) Use the Lookup tool to verify name & address resolutions and resolve any DNS problems.

   (3) Use Ping command to verify that the remote host is reachable.

   (4) If the remote host is unreachable, verify with the remote network manager that the remote host is operational.

   (5) If the remote host is operational, use the 'TraceRoute' command to locate any routing problems and inform the NOC of the problems.

c. Application Problem

   (1) The most likely causes of application problems are:
      - Remote server hardware is faulty;
      - Remote server software is badly configured; and/or

- Local client software is badly configured.

(2) Verify with the NOC that the remote server is operational and the local software configuration is correct. In coordination with the NOC resolve any configuration problems.

This page intentionally blank.

Annex B to Chapter 12 to ACP 200

OPTASK NET
(CONFIDENTIAL WHEN COMPLETED)

A1. **Purpose**

This OPTASK provides adequate information and direction to setup and configure a Maritime Tactical Wide Area Network (MTWAN).

A2. **Objective**

Provide maritime units operating with a multinational task group with the capability to maintain access to an allied tactical network.

B. **ADMINISTRATION**

B1. **Period**

Effective on order.

B2. **Scope**

Provide the technical information for the provision of an MTWAN including the setup, configuration, maintenance and management.

B3. **Change Management**

Proposed changes are to be forwarded to the AUSCANNZUKUS Permanent Secretary for staffing by AUSCANNZUKUS IAW ACP amendment procedures.

B4. **References**

B4.1. ACP 200 Networking at Sea
B4.2. OPTASK COMMS
B4.3. OPTASK KM
B4.4. OPTASK FOTC

C. **DUTIES**

C1. **CTG Network Manager**

C2. **NOC Manager**

C3. **Unit Network Manager**

D. **NAMING AND ADDRESSING**

D1. **Unit name**

D2. **IP address/Mask**

D3. **Multi-cast group and class D address**

D4. **DNS Root Server(s)**

D5. **Domain responsibility**

D5.1. Primary (Primary NOC/service.country/primary IP address/secondary IP address) (eg: MTWAN NOC/NAVY.US/A.B.C.D/A.B.C.D)

D6. **Host names and IP addresses**

E. **ROUTING**

E1. **AS number**

E2. **Bandwidth**

E3. **OSPF settings (area/dead time/hello interval/retransmit/cost)**

E4. **PIM settings (mode/ R/V point)**

F. **SUBNETS**

F1. **UHF SATCOM**

F1.1 CAP ID (unit/unique ID number)
F1.2 IP address/Mask (A.B.C.D/Hex)
F1.3 Baud rate
F1.4 Guard time
F1.5 Time Bytes
F1.6 Unique crypto settings

F2. **INMARSAT B**

F2.1 Unit/number
F2.2 IP address/Mask
F2.3 Baud rate
F2.4 Unique crypto settings

F3. **HF BLOS**

F3.1 CAP ID (unit/unique ID number)
F3.2 IP address/Mask (A.B.C.D/Hex)
F3.3 Modem mode
F3.4 Baud rate
F3.5 Interleave mode
F3.6 Transmit frequencies (ship freq/shore freq)
F3.7 Eval interval
F3.8 Unique crypto settings

F4. **IP 5066**

F4.1 Unit ID (unit/unique ID number)
F4.2 IP address/Mask (A.B.C.D/Hex)
F4.3 Modem mode
F4.4 Baud rate
F4.5 Interleave mode
F4.6 Transmit frequencies
F4.7 Unique crypto settings

G. **NETWORK MANAGEMENT**

G1. **Units are to report network status via local web services. NOC to provide URL.**

G2. **The NOC will maintain a 24/7 help desk to address network issues**

G3. **NOC telephone numbers.**

H. **APPLICATIONS**

H1. **Messaging**

H1.1 MSeG version nr
H1.2 Sendmail version nr
H1.3 Mx record
H1.4 Mailer table
H1.5 Multicast IP address
H1.6 Outbound configuration file
H1.7 MSeG configuration
H1.8 Sendmail.cf configuration

H2. **Common Operational Picture (COP)**

H2.1 MSeG version nr
H2.2 Multicast address
H2.3 Congestion control
H2.4 MSeG configuration

H3. **Web Services**

H3.1 Primary DOMINO server IP address
H3.2 DOMINO name structure
H3.3 Web browser version nr (specific version to be promulgated).

H4. **DCP**

H4.1 SAMETIME server IP address

H5. **Mchat**

H5.1 Version Nr
H5.2 Multicast address

H6. **ICE**

H6.1 Version nr

Appendix 1 to Annex B to Chapter 12 to ACP 200

OPTASK NET (Example)

(CONFIDENTIAL WHEN COMPLETED OUTSIDE OF ACP 200)

A1. **Purpose**

This OPTASK provides information and direction to setup and configure the networks in support of the MNTG for JWID 03.

A2. **Objective**

Provide maritime units operating with MNTG JWID 03 with the capability to maintain access to the JWID network(s).

B. **ADMINISTRATION**

B1. **Period**

Effective on order. Cancel upon completion of JWID 03 or when superceded.

B2. **Scope**

Provide the technical information for the provision of a MTWAN including the setup, configuration, maintenance and management.

B3. **Change Management**

Proposed changes to this OPTASK are to be forwarded to the CTG Network Manager for inclusion in an OPTASK NET Supplement or re-publishing.

B4. **References**

B4.1. ACP 200 Networking at Sea
B4.2. OPTASK COMMS
B4.3. OPTASK KM
B4.4. OPTASK FOTC

C. **DUTIES**

C1. **CTG Network Manager**

C1.1. The CTG Network Manager is responsible to the CTG for maintaining the good working of the networks under the CTG responsibility. He is also to collect and publish the following information daily at 1200Z:

C1.1.1. All network status
C1.1.2. Overall performance
C1.1.3. Network troubles if any
C1.1.4. Planned Network outage if any
C1.1.5. Misc. information

C1.2. The CTG Network Manager will follow the JWID 03 CTG rotation schedule.
C1.3. Any other duties???

C2. **NOC Network Manager**

C2.1. The NOC Network Manager is responsible for network maintenance. This includes establishment and monitoring of networks to support MNTG, and customer service support.
C2.2. The NOC Network Manager is also responsible to the CTG to provide IP addresses to units requiring them via an OPTASK NET supplement containing all pertinent information.
C2.3. The following personnel will be acting as NOC Network Manager for JWID 03. They are the primary point of contacts for their respective NOC read in 4 columns: country/poc/phone number/e-mail

a-aus/Mr. Van Vu/612 6266 3217/van.vu@defence.gov.au
b-ca/Lt(N) Mario Bernier/819 994 8487/Bernier.M@forces.gc.ca
c-nz/Lt Mike Deureyter/
d-uk/Mr. Andrew Checker/
e-us/Ms. Anh Nguyen/619 553 /

C3. **Unit Network Manager**

C3.1. The unit Network Manager is responsible to his CO for the maintaining and good functioning of the Network under the CO responsibility. He is also responsible to the CTG Network Manager to report the network status and deficiencies.
C3.3. The following personnel will be acting as Unit Network Manager for JWID 03. They are the primary point of contacts for their respective units read in 4 columns: country/poc/phone number/e-mail:

a-aus/Mr. Van Vu/612 6266 3217/van.vu@defence.gov.au
b-ca/Lt(N) Mario Bernier/819 994 8487/Bernier.M@forces.gc.ca

c-nz/Lt Mike Deureyter/
d-uk/Mr. Andrew Checker/
e-us/Ms. Anh Nguyen/619 553 /

D. **NAMING AND ADDRESSING**

D1. **Unit name**

D1.1. Unit names are as follows (All countries to report the proper 3 letter desig for their respective units). Read in 2 columns: unit/letters desig :

D1.1.1. AU NOC/aunoc
D1.1.2. HMAS Canberra/can
D1.1.3. HMAS Manoora/man
D1.1.4. HMAS Robertson/rob
D1.1.5. CA NRS Bras D'Or/nrsbdo
D1.1.6. HMCS Coaticook/coa
D1.1.7. HMCS Renfrew/ren
D1.1.8. NZ NOC/nznoc
D1.1.9. HMNZS Waka/wak
D1.1.10. UK NOC/noc
D1.1.11. HMS Albion/alb
D1.1.12. HMS Ocean/oce
D1.1.13. HMS Illustrious/ill
D1.1.14. UK 3 CDO BDE/uk3cdo
D1.1.15. UK 40 CDO/uk40cdo
D1.1.16. US NRS/nrssd
D1.1.17. USS Bataan/bat
D1.1.18. USS Paul Hamilton/pha

D2. **IP address/Mask**

Following IP addresses/Netmasks are effective for the duration of JWID 03. Read in 4 columns: unit/network/netmasks/broadcast.

D2.1 Australia

a-NOC/xxx.xxx.42.0/255.255.255.240/xxx.xxx.42.15
b-HMAS Canberra/xxx.xxx.42.16/255.255.255.240/xxx.xxx.42.31
c-HMAS Manoora/xxx.xxx.42.32/255.255.255.240/xxx.xxx.42.47
d-HMAS Sydney/xxx.xxx.42.48/255.255.255.240/xxx.xxx.42.63
e-Spare/xxx.xxx.42.64/255.255.255.240/xxx.xxx.42.79
f-Spare/xxx.xxx.42.80/255.255.255.240/xxx.xxx.42.95

g-Spare/xxx.xxx.42.96/255.255.255.240/xxx.xxx.42.111

D2.2. Canada

a-NRS Bras D'Or/xxx.xxx.192.0/255.255.255.0/xxx.xxx.192.255
b-HMCS Coaticook/255.255/255.0/xxx.xxx.194.255
c-HMCS Renfrew/255.255.255.0/xxx.xxx.196.255

D2.3. New Zealand

a-NZ NOC/xxx.xxx.42.128/255.255.255.240/xxx.xxx.42.143
b-HMNZS Te Mana/xxx.xxx.42.144/255.255.255.240/xxx.xxx.42.159
c-NZ FE/xxx.xxx.42.160/255.255.255.240/xxx.xxx.42.175
d-Spare/xxx.xxx.42.176/255.255.255.240/xxx.xxx.42.191
e-Spare/xxx.xxx.42.192/255.255.255.240/xxx.xxx.42.207
f-Spare/xxx.xxx.42.208/255.255.255.240/xxx.xxx.42.223
g-Spare/xxx.xxx.42.224/255.255.255.240/xxx.xxx.42.239
h-Spare/xxx.xxx.42.240/255.255.255.240/xxx.xxx.42.255

D2.4 United Kingdom

a-UK NOC/25.

D2.5. United States

a-NRS SD/xxx.xxx.43.0/255.255.255.240/xxx.xxx.43.15
b-USS Bataanxxx.xxx.43.16/255.255.255.240/xxx.xxx.43.31
c-USS Paul Hamiltonxxx.xxx.43.32/255.255.255.240/xxx.xxx.43.47
d-USMC Det/xxx.xxx.43.48/255.255.255.240/xxx.xxx.43.63
e-Spare/xxx.xxx.43.64/255.255.255.240/xxx.xxx.43.79
f-Spare/xxx.xxx.43.80/255.255.255.240/xxx.xxx.43.95
g-Spare/xxx.xxx.43.96/255.255.255.240/xxx.xxx.43.111
h-Spare/xxx.xxx.43.112/255.255.255.240/xxx.xxx.43.127
j-Spare/xxx.xxx.43.128/255.255.255.240/xxx.xxx.43.143
k-Spare/xxx.xxx.43.144/255.255.255.240/xxx.xxx.43.159
l-Spare/xxx.xxx.43.160/255.255.255.240/xxx.xxx.43.175
m-Spare/xxx.xxx.43.176/255.255.255.240/xxx.xxx.43.191
n-Spare/xxx.xxx.43.192/255.255.255.240/xxx.xxx.43.207
o-Spare/xxx.xxx.43.208/255.255.255.240/xxx.xxx.43.223
p-Spare/xxx.xxx.43.224/255.255.255.240/xxx.xxx.43.239
q-Spare/xxx.xxx.43.240/255.255.255.240/xxx.xxx.43.255

D3. **Multi-cast group and class D address**

D3.1. Following Class D address groups will be used during JWID 03. Read in 3 columns: group name/IP address/port number.

a-MSEG (fast)/224.100.100.11/5011
b-MSEG (slow)/224.100.100.12/5012
c-AU MNTG NOC/224.100.100.21/5021
d-HMAS MANOORA/224.100.100.22/5022
e-HMAS ROBERTSON/224.100.100.23/5023
f-HMAS CANBERRA/224.100.100.24/5024
g-HMCS COATICOOK/224.100.100.25/5025
h-HMCS RENFREW/224.100.100.26/5026
j-NRS BRAS D'OR/224.100.100.27/5027
k-NRS RENFREW/224.100.100.28/5028
l-NZ TAC NOC/224.100.100.29/5029
m-HMNZS WAKA/224.100.100.30/5030
n-UK MNTG NOC/224.100.100.31/5031
o-HMS ALBION/224.100.100.32/5032
p-RFA ARGUS/224.100.100.33/5033
q-HMS OCEAN/224.100.100.34/5034
r-UK 40 Commando/224.100.100.35/5035
s-NRS SSCSD/224.100.100.36/5036
t-USS BATAAN/224.100.100.37/5037
u-USS PAUL HAMILTON/224.100.100.38/5038

D4. **DNS Root Server(s)**

D4.1.

a-./999999999/IN/NS/root1.
a.1-root1. /999999999/IN/A/ xxx.xxx.48.20
b-./999999999/IN/NS/root2.
b.1-root2./999999999/IN/A/ xxx.xxx.248.10
c-./999999999/IN/NS/root3.
c.1-root3./999999999/IN/A/ xxx.xxx.8.10
d-./999999999/IN/NS/root4.
d.1-root4./999999999/IN/A/ xxx.xxx.8.20

D5. **Domain responsibility**

D5.1. Primary (Primary NOC/service.country/primary IP address/secondary IP address) (eg: MTWAN NOC/NAVY.US/A.B.C.D/A.B.C.D)

a-AUS NOC/navy.au/xxx.xxx.42.2/xxx.xxx.43.21
b-CA NOC/navy.ca/xxx.xxx.192.20/xxx.xxx.43.21
c-NZ NOC/navy.nz/xxx.xxx.43.133/xxx.xxx.43.21
d-UK NOC/navy.uk/xxx.xxx.ccc.ddd/aaa.bbb.ccc.ddd
e-US NOC/navy.us/xxx.xxx.43.21/xxx.xxx.192.20
f-US NOC/usmc.us/xxx.xxx.43.21/xxx.xxx.192.20

D6. **Host names and IP addresses**

Only major host are listed in this para. Read in 4 columns: Function/Hostname/IP Address/Netmask (These addresses must be compared against the official JWID 03 addressing plan. Following IPs used as filler)

D6.1. AUSTRALIA

D6.1.1. HMAS Robertson

a-Gccs-m/goanna.robertson.navy.au/xxx.xxx.43.1/255.255.255.240
b-General Server/emu.robertson.navy.au/xxx.xxx.43.2/255.255.255.240
c-C2pc/possum.robertson.navy.au/xxx.xxx.43.4/255.255.255.240
d-Domino/wombat.robertson.navy.au/xxx.xxx.43.5/255.255.255.240
e-HF BLOS CAP/hfbloscap.robertson.navy.au/xxx.xxx.43.10/255.255.255.240
f-UHF SATCOM CAP/uhfcap.robertson.navy.au/xxx.xxx.43.11/255.255.255.240
g-Router/gateway.robertson.navy.au/xxx.xxx.43.13/255.255.255.240
h-Printer/gum.robertson.navy.au/xxx.xxx.43.14/255.255.255.240

D6.1.2. HMAS Manoora

a-Gccs-m/bream.manoora.navy.au/xxx.xxx.43.17/255.255.255.240
b-General Server/galah.manoora.navy.au/xxx.xxx.43.18/255.255.255.240
c-Domino/bogong.manoora.navy.au/xxx.xxx.43.20/255.255.255.240
d-HF BLOS CAP/hfbloscap.manoora.navy.au/xxx.xxx.43.26/255.255.255.240
e-UHF SATCOM CAP/uhfcap.manoora.navy.au/xxx.xxx.43.27/255.255.255.240
g-Router/gateway.manoora.navy.au/xxx.xxx.43.29/255.255.255.240

D6.1.3. HMAS Canberra

a-Gccs-m/goanna.canberra.navy.au/xxx.xxx.43.1/255.255.255.240
b-General Server/emu.canberra.navy.au/xxx.xxx.43.2/255.255.255.240
c-C2pc/possum.canberra.navy.au/xxx.xxx.43.4/255.255.255.240
d-Domino/wombat.canberra.navy.au/xxx.xxx.43.5/255.255.255.240
e-HF BLOS CAP/hfbloscap.canberra.navy.au/xxx.xxx.43.10/255.255.255.240
g-UHF SATCOM CAP/uhfcap.canberra.navy.au/xxx.xxx.43.11/255.255.255.240
h-Router/gateway.canberra.navy.au/xxx.xxx.43.13/255.255.255.240

D6.1.4. AUS NOC

a-Gccs-m/goanna.aunoc.navy.au/xxx.xxx.43.1/255.255.255.240
b-General Server/emu.aunoc.navy.au/xxx.xxx.43.2/255.255.255.240
c-C2pc/possum.aunoc.navy.au/xxx.xxx.43.4/255.255.255.240
d-Domino/wombat.aunoc.navy.au/xxx.xxx.43.5/255.255.255.240
e-HF BLOS CAP/hfbloscap.aunoc.navy.au/xxx.xxx.43.10/255.255.255.240
f-UHF SATCOM CAP/uhfcap.aunoc.navy.au/xxx.xxx.43.11/255.255.255.240
g-Router/gateway.aunoc.navy.au/xxx.xxx.43.13/255.255.255.240

D6.2. CANADA

D6.2.1. NRS Bras D'Or

a-Router/gateway.nrsbdo.navy.ca/xxx.xxx.248.1/255.255.255.0
b-Time server/time-serv.nrsbdo.navy.ca/xxx.xxx.248.2/255.255.255.0
c-General server/dns.nrsbdo.navy.ca/xxx.xxx.248.3/255.255.255.0
d-Mseg/mseg.nrsbdo.navy.ca/xxx.xxx.248.3/255.255.255.0
e-Domino/domino.nrsbdo.navy.ca/xxx.xxx.248.4/255.255.255.0
f-GCCS-M/gccsm.nrsbdo.navy.ca/xxx.xxx.248.5/255.255.255.0
g-Cisco Call Manager/ccm.nrsbdo.navy.ca/xxx.xxx.248.6/255.255.255.0
h-IP Phone/phone.nrsbdo.navy.ca/xxx.xxx.248.9/255.255.255.0
j-SNR/snr.nrsbdo.navy.caxxx.xxx.248.248

D6.2.2. HMCS Coaticook

a-Router/gateway.coa.navy.ca/xxx.xxx.248.1/255.255.255.0
b-Time server/time-serv.coa.navy.ca/xxx.xxx.248.2/255.255.255.0
c-General server/dns.coa.navy.ca/xxx.xxx.248.3/255.255.255.0
d-Mseg/mseg.coa.navy.ca/xxx.xxx.248.3/255.255.255.0
e-Domino/domino.coa.navy.ca/xxx.xxx.248.4/255.255.255.0
f-GCCS-M/gccsm.coa.navy.ca/xxx.xxx.248.5/255.255.255.0
g-IP Phone/phone.coa.navy.ca/xxx.xxx.248.9/255.255.255.0
h-SNR/snr.coa.navy.caxxx.xxx.248.248

D6.2.3. HMCS Renfrew

a-Router/gateway.ren.navy.ca/xxx.xxx.248.1/255.255.255.0
b-Time server/time-serv.ren.navy.ca/xxx.xxx.248.2/255.255.255.0
c-General server/dns.ren.navy.ca/xxx.xxx.248.3/255.255.255.0
d-Mseg/mseg.ren.navy.ca/xxx.xxx.248.3/255.255.255.0
e-Domino/domino.ren.navy.ca/xxx.xxx.248.4/255.255.255.0
f-GCCS-M/gccsm.ren.navy.ca/xxx.xxx.248.5/255.255.255.0
g-IP Phone/phone.ren.navy.ca/xxx.xxx.248.9/255.255.255.0

h-SNR/snr.ren.navy.caxxx.xxx.248.248

D6.3. NEW ZEALAND

D6.3.1. NZ NOC

a-Router/rout.nznoc.navy.nz/xxx.xxx.42.65/255.255.255.240
b-GCCS-M/gccs.nznoc.navy.nz/xxx.xxx.42.66/255.255.255.240
c-Domino Server/dom.nznoc.navy.nz/xxx.xxx.42.67/255.255.255.240
d-Sun Sparc/gen1.nznoc.navy.nz/xxx.xxx.42.69/255.255.255.240

D6.3.2. HMNZS Waka

a-Router/rout.waka.navy.nz/xxx.xxx.42.81/255.255.255.240
b-GCCS-M/gccs.waka.navy.nz/xxx.xxx.42.83/255.255.255.240
c-Domino Server/dom.waka.navy.nz/xxx.xxx.42.84/255.255.255.240
d-Sun Sparc/gen1.waka.navy.nz/xxx.xxx.42.86/255.255.255.240
e-Cap/cap.waka.navy.nz/xxx.xxx.42.88/255.255.255.240
f-Criu/criu.waka.navy.nz/xxx.xxx.42.89/255.255.255.240

D6.4. United Kingdom

D6.4.1. UK NOC

a-Router/rout.uknoc.navy.uk/xxx.xxx.42.81/255.255.255.240
b-GCCS-M/gccs.uknoc.navy.uk/xxx.xxx.42.83/255.255.255.240
c-Domino Server/dom.uknoc.navy.uk/xxx.xxx.42.84/255.255.255.240
d-Sun Sparc/gen1.uknoc.navy.uk/xxx.xxx.42.86/255.255.255.240
f-Cap/cap.uknoc.navy.uk/xxx.xxx.42.88/255.255.255.240
g-Criu/criu.uknoc.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.4.2. HMS ALBION

a-Router/rout.alb.navy.uk/xxx.xxx.42.81/255.255.255.240
b-GCCS-M/gccs.alb.navy.uk/xxx.xxx.42.83/255.255.255.240
c-Domino Server/dom.alb.navy.uk/xxx.xxx.42.84/255.255.255.240
d-Sun Sparc/gen1.alb.navy.uk/xxx.xxx.42.86/255.255.255.240
f-Cap/cap.alb.navy.uk/xxx.xxx.42.88/255.255.255.240
g-Criu/criu.alb.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.4.3. RFA ARGUS

a-Router/rout.arg.navy.uk/xxx.xxx.42.81/255.255.255.240

b-GCCS-M/gccs.arg.navy.uk/xxx.xxx.42.83/255.255.255.240
c-Domino Server/dom.arg.navy.uk/xxx.xxx.42.84/255.255.255.240
d-Sun Sparc/gen1.arg.navy.uk/xxx.xxx.42.86/255.255.255.240
f-Cap/cap.arg.navy.uk/xxx.xxx.42.88/255.255.255.240
g-Criu/criu.arg.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.4.4. HMS OCEAN

a-Router/rout.oce.navy.uk/xxx.xxx.42.81/255.255.255.240
b-GCCS-M/gccs.oce.navy.uk/xxx.xxx.42.83/255.255.255.240
c-Domino Server/dom.oce.navy.uk/xxx.xxx.42.84/255.255.255.240
d-Sun Sparc/gen1.oce.navy.uk/xxx.xxx.42.86/255.255.255.240
f-Cap/cap.oce.navy.uk/xxx.xxx.42.88/255.255.255.240
g-Criu/criu.oce.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.4.5. HMS TBD

a-Router/rout.tbd.navy.uk/xxx.xxx.42.81/255.255.255.240
b-GCCS-M/gccs.tbd.navy.uk/xxx.xxx.42.83/255.255.255.240
c-Domino Server/dom.tbd.navy.uk/xxx.xxx.42.84/255.255.255.240
d-Sun Sparc/gen1.tbd.navy.uk/xxx.xxx.42.86/255.255.255.240
f-Cap/cap.tbd.navy.uk/xxx.xxx.42.88/255.255.255.240
g-Criu/criu.tbd.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.4.6. UK 40 CDO

a-Router/rout.uk40cdo.navy.uk/xxx.xxx.42.81/255.255.255.240
b-GCCS-M/gccs.uk40cdo.navy.uk/xxx.xxx.42.83/255.255.255.240
c-Domino Server/dom.uk40cdo.navy.uk/xxx.xxx.42.84/255.255.255.240
d-Sun Sparc/gen1.uk40cdo.navy.uk/xxx.xxx.42.86/255.255.255.240
f-Cap/cap.uk40cdo.navy.uk/xxx.xxx.42.88/255.255.255.240
g-Criu/criu.uk40cdo.navy.uk/xxx.xxx.42.89/255.255.255.240

D6.5. United States

D6.5.1. NRS San Diego

a-router/rout.nrssd.navy.us/xxx.xxx.43.17/255.255.255.240
b-Whatsup/whatsup.nrssd.navy.us/xxx.xxx.43.19/255.255.255.240
c-JMUG/jmug.nrssd.navy.us/xxx.xxx.43.21/255.255.255.240
d-DNS/jmug.nrssd.navy.us/xxx.xxx.43.21/255.255.255.240
e-PMUL/pmul.nrssd.navy.us/xxx.xxx.43.22/255.255.255.240

f-Domino/domino.nrssd.navy.us/xxx.xxx.43.24/255.255.255.240
g-Sametime/sametime.nrssd.navy.us/xxx.xxx.43.25/255.255.255.240
h-Taclane/taclane.nrssd.navy.us/xxx.xxx.43.27/255.255.255.240
j-UHF-CAP1/uhf-cap1.nrssd.navy.us/xxx.xxx.43.29/255.255.255.240
k-CRIU/uhf-criu.nrssd.navy.us/xxx.xxx.43.30/255.255.255.240

D6.5.2. USS Bataan

a-Router/rout.bat.navy.us/xxx.xxx.43.49/255.255.255.240
b-Whatsup/whatsup.bat.navy.us/xxx.xxx.43.50/255.255.255.240
c-JMUG/jmug.bat.navy.us/xxx.xxx.43.52/255.255.255.240
d-DNS/jmug.bat.navy.us/xxx.xxx.43.52/255.255.255.240
e-Intel/intel.bat.navy.us/xxx.xxx.43.54/255.255.255.240
f-Ops/ops.bat.navy.us/xxx.xxx.43.55/255.255.255.240
g-GCCS-M/gccsm.bat.navy.us/xxx.xxx.43.56/255.255.255.240
h-Domino/domino.bat.navy.us/xxx.xxx.43.57/255.255.255.240
j-Taclane/taclane.bat.navy.us/xxx.xxx.43.60/255.255.255.240
k-bridge1/bridge1.bat.navy.us/xxx.xxx.43.61/255.255.255.240
l-bridge2/bridge2.bat.navy.us/xxx.xxx.43.62/255.255.255.240

D6.5.3. USS Paul Hamilton

a-Router/rout.pha.navy.us/xxx.xxx.43.49/255.255.255.240
b-Whatsup/whatsup.pha.navy.us/xxx.xxx.43.50/255.255.255.240
c-JMUG/jmug.pha.navy.us/xxx.xxx.43.52/255.255.255.240
d-DNS/jmug.pha.navy.us/xxx.xxx.43.52/255.255.255.240
e-Intel/intel.pha.navy.us/xxx.xxx.43.54/255.255.255.240
f-Ops/ops.pha.navy.us/xxx.xxx.43.55/255.255.255.240
g-GCCS-M/gccsm.pha.navy.us/xxx.xxx.43.56/255.255.255.240
h-Domino/domino.pha.navy.us/xxx.xxx.43.57/255.255.255.240
j-Taclane/taclane.pha.navy.us/xxx.xxx.43.60/255.255.255.240
k-bridge1/bridge1.pha.navy.us/xxx.xxx.43.61/255.255.255.240
l-bridge2/bridge2.pha.navy.us/xxx.xxx.43.62/255.255.255.240

D6.5.4. US Marine Corps

a-Router/gateway.31meu.usmc.us/xxx.xxx.43.129/255.255.255.224
b-Domino/domino.31meu.usmc.us/xxx.xxx.43.130/255.255.255.224
c-MIDB/ias.31meu.usmc.us/xxx.xxx.43.131/255.255.255.224
d-Printer/printer.31meu.usmc.us/xxx.xxx.43.132/255.255.255.224
e-C2PC/nt1mntg.31meu.usmc.us/xxx.xxx.43.133/255.255.255.224
f-C2PC/nt2mntg.31meu.usmc.us/xxx.xxx.43.134/255.255.255.224

g-GCCS/mntgcop.31meu.usmc.us/xxx.xxx.43.135/255.255.255.224
h-C2PC/nt3mntg.31meu.usmc.us/xxx.xxx.43.136/255.255.255.224
j-C2PC/nt4mntg.31meu.usmc.us/xxx.xxx.43.137/255.255.255.224
k-C2PC/nt5mntg.31meu.usmc.us/xxx.xxx.43.138/255.255.255.224
l-C2PC/nt6mntg.31meu.usmc.us/xxx.xxx.43.139/255.255.255.224

E. **ROUTING**

E1. **AS number**

Following Autonomous System area number will be effective fro the duration of JWID 03. Read in 3 columns: country/network/AS number.

a-Australia/MNTG/1011
b-Canada/MNTG/1012
c-New Zealand/MNTG/1013
d-United Kingdom/MNTG/1014
e-United States/MNTG/1015

E2. **Bandwidth**

E2.1. SHF

a-128 kbps

E2.2. INMARSAT B

a-128 kbps dual
b-64 kbps

E2.3. UHF SATCOM

a-6 kbps/32 kbps 5 members net
b-4.8 kbps/ 16 kbps 3 members net

E2.4. HF BLOS

a-19.2 kbps 110b coded waveform
b-9.6 kbps 110b coded waveform
c-2.4 kbps 4285 coded waveform

E2.5. SNR UHF LOS

a-41 kbps at 78.6 kbps single net with 6 members
b-34 kbps at 78.6 kbps in-line topology with 4 relays
c-20 kbps at 78.6 kbps 2 nets with 1 relay

E3. **OSPF settings (bw in kbps/area/dead time/hello interval/retransmit/cost)**

E3.1. SHF

a-128/0/40/10/5/800

E3.2. INMARSAT

a-128/0/40/10/5/750
b-64/0/40/10/5/750

E3.3. UHF SATCOM

E3.1 5Khz Channel

a-2.4/0/120/30/10/3400
b-4.8/0/120/30/10/2660
c-9.6/0/120/30/10/2220

E.3.2 25Khz Channel

a-16/0/120/30/10/1500
b-32/0/120/30/10/1300
c-38.4/0/120/30/10/1250
d-48/0/120/30/10/1200
e-56/0/120/30/10/1150

E3.4. HF BLOS

a-19.2/0/120/30/10/1500
b.9.6/0/120/30/10/1900
c-2.4/0/120/30/10/3200

E3.5. SNR UHF LOS

a-78.6/0/40/10/5/1125
b-64/0/40/10/5/1150
c-32/0/40/10/5/1300

E4. **PIM settings (mode/ R/V point/priority)**

E4.1. AU NOC

a-sparse-dense/xxx.xxx.421/50

E4.2. CA NOC

a-sparse-dense/xxx.xxx.192.1/100

E4.3. NZ NOC

a-sparse-dense/xxx.xxx.42.129/50

E4.4. UK NOC

a-sparse-dense/xxx.xxx.ccc.ddd/50

E4.5. US NOC

a-sparse-dense/xxx.xxx.43.1/100

F. **SUBNETS**

F1. **UHF SATCOM**

F1.1 Router Interface IP
F1.2 IP address/Mask (A.B.C.D/Hex)
F1.3 Baud rate
F1.4 Guard time
F1.5 Time Bytes
F1.6 Unique crypto settings

F2. **INMARSAT B**

F2.1 Unit/number
F2.2 IP address/Mask
F2.3 Baud rate
F2.4 Unique crypto settings

F3. **HF BLOS**

F3.1 CAP ID (unit/unique ID number)
F3.2 IP address/Mask (A.B.C.D/Hex)

F3.3 Modem mode
F3.4 Baud rate
F3.5 Interleave mode
F3.6 Transmit frequencies (ship freq/shore freq)
F3.7 Eval interval
F3.8 Unique crypto settings

F4. **IP 5066**

F4.1 Unit ID (unit/unique ID number)
F4.2 IP address/Mask (A.B.C.D/Hex)
F4.3 Modem mode
F4.4 Baud rate
F4.5 Interleave mode
F4.6 Transmit frequencies
F4.7 Unique crypto settings

G. **NETWORK MANAGEMENT**

G1. **Units are to report network status via local web services. NOC to provide URL.**

G2. **The NOC will maintain a 24/7 help desk to address network issues**

G3. **NOC telephone numbers.**

H. **APPLICATIONS**

H1. **Messaging**

H1.1 MSE version nr
H1.2 Sendmail version nr
H1.3 Mx record
H1.4 Mailer table
H1.5 Multicast IP address
H1.6 Outbound configuration file
H1.7 P_Mul configuration
H1.8 Sendmail.cf configuration

H2. **Common Operational Picture (COP)**

H2.1 MSEG version nr
H2.2 Multicast address

H2.3 Congestion control
H2.4 MSEG configuration

H3. **Web Services**

H3.1 Primary DOMINO server IP address
H3.2 Domino Replication Topology
H3.3 DOMINO name structure
H3.4 Address Book
H3.5 Web browser version nr (specific version to be promulgated).

H4. **DCP**

H4.1 SAMETIME server IP address

H5. **MSEG**

H5.1 Version Nr
H5.2 Multicast address

H6. **ICE**

H6.1 Version nr

This page intentionally blank.